

PROCEDE ET DISPOSITIF ASSOCIE DE GENERATION DE NOMBRES ALEATOIRES
DANS UN INTERVALLE DONNE

L'invention concerne un procédé d'obtention d'un nombre aléatoire compris entre A et B à partir d'un générateur produisant des nombres aléatoires compris entre 0 et W-1, avec N la taille des nombres produits par le générateur, W-1 la valeur maximale prise par les nombres aléatoires produits, avec par exemple $W = 2^N$, et A, B des nombres entiers quelconques, inférieurs ou supérieurs au nombre W.

Une telle situation se produit par exemple dans un composant électronique adapté pour réaliser des calculs cryptographiques et comprenant un générateur de nombres aléatoires de N bits, par exemple $N = 8$. Les nombres aléatoires qu'il peut produire sont ainsi compris entre 0 et $W-1 = 255$, alors qu'il serait souhaitable de disposer de nombres aléatoires compris par exemple entre 0 et 100 ou entre 300 et 10000. A noter qu'il suffit de déterminer des nombres entre 0 et 9700 puis d'ajouter ensuite 300 au nombre obtenu pour obtenir finalement un nombre entre 300 et 10000.

Une telle situation se retrouve dans la pratique dans la plupart des applications cryptographiques, par exemple la signature DSA, la signature ou le chiffrement d'El Gamal, le développement de contremesures contre diverses attaques, etc.

Plusieurs procédés sont déjà connus pour produire des nombres aléatoires R compris entre 0 et K à partir de nombres compris entre 0 et W-1. Ces procédés sont en général mis en œuvre par des moyens logiciels utilisés

pour piloter d'une part un générateur hardware qui produit des nombres aléatoires de taille N et d'autre part des moyens de calcul réalisant notamment des opérations de multiplications, d'additions, etc.

Un premier procédé connu comprend les étapes suivantes :

- a) déterminer le plus petit nombre entier p tel que $K \leq W^p - 1$,
- b) produire p nombres aléatoires S_0, S_1, \dots, S_{p-1} et former la variable $S = \sum_{i=0}^{p-1} S_i * W^i$
- c) si $S > K$, alors retourner à l'étape b), sinon poser $R = S$

R est le nombre aléatoire recherché, compris entre 0 et K. L'équation $S = \sum_{i=0}^{p-1} S_i * W^i$ est une représentation de la variable S décomposée / recomposée dans la base $(W^{p-1}, \dots, W^1, W^0)$. On pourrait également noter $S = S_{p-1}S_{p-2}\dots S_1S_0$, notation couramment utilisée.

Un deuxième procédé connu comprend les étapes suivantes :

- a) déterminer le plus petit nombre entier p tel que $K \leq W^p - 1$,
- b) produire p nombres aléatoires S_0, S_1, \dots, S_{p-1} et former la variable $T = \sum_{i=0}^{p-2} S_i * W^i$ et $S = T + S_{p-1} * W^{p-1}$
- c) si $S > K$, poser $R = T$, sinon poser $R = S$.

Un troisième procédé connu comprend les étapes suivantes :

- a) déterminer le plus petit nombre entier p tel que $K \leq W^p - 1$,

- b) produire p nombres aléatoires S_0, S_1, \dots, S_{p-1} et former la variable $S = \sum_{i=0}^{p-1} S_i * W^i$
- c) poser $R = S \bmod(K+1)$, c'est-à-dire le reste de la division entière de S par K+1, également appelé réduction modulaire de S par K+1.

Ces trois procédés peuvent être résumés par les étapes suivantes :

- a) produire p nombres aléatoires S_0, S_1, \dots, S_{p-1} , p étant le plus petit nombre entier tel que $K \leq W^p - 1$, et former la variable $S = \sum_{i=0}^{p-1} S_i * W^i$
- b) déterminer le nombre aléatoire R à partir de la variable S.

Selon le cas, au cours de l'étape b, on obtient R à partir de S en répétant l'étape b (1^{er} procédé), en tenant compte ou non du nombre aléatoire supplémentaire S_{p-1} (2^{ème} procédé) ou en effectuant une réduction modulaire (3^{ème} procédé).

A noter que, dans les trois procédés, si un nombre compris entre A et K+A est souhaité, il suffit d'ajouter A au nombre R obtenu compris entre 0 et K.

Le premier procédé a pour principal inconvénient un temps de calcul particulièrement long et surtout imprévisible : l'étape de production des p nombres aléatoires peut être répétée de nombreuses fois sans qu'il soit possible de prévoir au départ le nombre de répétitions de cette étape.

Le 2^{ème} et le 3^{ème} procédés ont pour principal inconvénient de produire des nombres aléatoires présentant un biais : parmi les nombres R produits dans l'intervalle $[0, K]$,

certaines valeurs sont plus probables que d'autres. Dit autrement, les nombres R produits ne sont pas parfaitement aléatoires (distribution non uniforme). Ce biais peut avoir des conséquences importantes sur la sécurité des systèmes cryptographiques susceptibles de mettre en œuvre ces procédés. La sécurité des systèmes cryptographiques suppose en effet que les nombres aléatoires qu'ils utilisent soient uniformément distribués (ou au moins proches d'une distribution uniforme) dans l'intervalle $[0, K]$ ou $[A, K+A]$ souhaité.

Enfin, les trois procédés sont globalement lents parce qu'ils mettent en œuvre des opérations sur des grands nombres, de taille N (au sens nombre de bits) supérieure à la taille des circuits utilisés pour la mise en œuvre. En effet, le nombre K notamment, est quelconque et peut être supérieur à W et donc de taille supérieure à N . La variable S peut également être de grande taille. Or, la mise en œuvre d'opérations sur des grands nombres nécessite la mise en œuvre de procédés complexes et coûteux en termes de temps de calcul.

Un objet essentiel de l'invention est de proposer un procédé de construction d'un nombre aléatoire R particulièrement rapide.

Ainsi, l'invention propose un procédé cryptographique, au cours duquel on utilise un générateur de nombres aléatoires produisant des nombres aléatoires S_i de taille N fixée compris entre 0 et $W-1$, avec par exemple mais non nécessairement $W = 2^N$, pour produire un nombre aléatoire R compris entre 0 et une borne K prédéfinie.

Les étapes essentielles d'un procédé selon l'invention sont les suivantes :

E31 : on produit une variable aléatoire S_i comprise entre 0 et $W-1$,

E32 : si la variable aléatoire S_i est strictement inférieure à un coefficient K_i de la borne K dans la base W , alors le coefficient R_i de rang i du nombre aléatoire R est égal à la variable aléatoire S_i puis, pour tout rang j inférieur à i , on produit une variable aléatoire S_j entre 0 et $W-1$ et on pose $R_j = S_j$.

E33 : sinon, si la dite variable aléatoire est supérieure au coefficient K_i de rang i de la borne K dans la base W , alors on détermine le dit coefficient R_i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie, puis on détermine le coefficient R_{i-1} du nombre aléatoire R de rang $i-1$ immédiatement inférieur en répétant les étapes E31 à E33.

Ainsi, dans un procédé selon l'invention, on recherche un à un les coefficients R_i du nombre aléatoire R souhaité, en commençant par le coefficient R_{p-1} le plus significatif. Le générateur physique de nombres aléatoires utilisés produit ainsi des variables aléatoires S_i une à une, une variable à chaque itération.

De plus, le procédé est rapide car l'étape E33 est exécutée un nombre restreint de fois. En effet, dès qu'une des variables S_i produite par le générateur physique est inférieure au coefficient K_i associé de la borne K , le procédé ne nécessite plus le traitement des variables S_j de rang inférieur à i : on calcule ainsi le

plus souvent un nombre restreint de coefficients du nombre R, les plus significatifs.

Enfin, par rapport aux procédés connus, un procédé selon l'invention présente l'avantage de travailler sur des nombres de au plus N bits, N étant la taille des registres et autres circuits de calculs des dispositifs utilisés pour la mise en œuvre. Par exemple, si W est égal à 2^N , les coefficients K_i , résultant de la décomposition de K dans la base $(W^{p-1}, \dots, W^1, W^0)$, sont nécessairement inférieurs à W et donc de taille au plus N bits. De même, les variables aléatoires S_i produites par le générateur physique de nombres aléatoires sont également de N bits.

En ajoutant aux étapes essentielles une étape d'initialisation et une étape de recombinaison du nombre aléatoire R, on obtient :

E1 : on décompose la borne K dans une base $(W^{p-1}, W^{p-2}, \dots, W^0)$ ($K = \sum_{i=0}^{p-1} K_i * W^i$ ou $K = K^{p-1} \dots K^1 K^0$), i étant un

indice de boucle, K_i étant un coefficient de la borne K de rang i compris entre 0 et W-1 et p étant le degré de la borne K,

E2 : on initialise à VRAI une variable booléenne f,

E3 : on réalise les opération suivantes, dans une boucle indicée par i, i étant un nombre entier variant entre p-1 et 0:

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure au coefficient K_i de rang i, alors on met à FAUX la variable booléenne f,

E33_1 : si la variable aléatoire S_i est strictement supérieure au coefficient K_i de rang i et si la variable booléenne f est VRAI, alors on détermine le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie,

E33_2 : sinon, on pose $R_i = S_i$

E34 : on décrémente l'indice de boucle i ,

E4 : on détermine le nombre aléatoire R par recombinaison des coefficients aléatoires R_i dans la base W ($R = \sum_{i=0}^{P-1} R_i * W^i$ ou $R^{P-1}...R^1R^0$).

Concrètement, dès que la variable booléenne f est positionnée à FAUX, elle reste à cette valeur, puisqu'il n'est pas prévu de la repositionner à la valeur VRAI, sauf lors de l'initialisation E2 du procédé. L'étape E33 est exécutée uniquement si la variable f est VRAI ; ainsi, dès que la variable f est positionnée à la valeur FAUX, l'étape E33_1 n'est plus exécutée et le procédé selon l'invention se termine rapidement.

Un deuxième objectif de l'invention est de proposer un procédé de construction de nombres aléatoires dont la distribution soit uniforme ou puisse être rendue aussi proche que souhaitée d'une distribution uniforme. Cet objectif est atteint en choisissant une fonction adéquate pour la détermination du coefficient R_i à partir de la variable aléatoire S_i .

Selon un premier mode de mise en œuvre d'un procédé selon l'invention, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33_1), on réalise les sous-étapes suivantes :

E33_11: si la variable aléatoire S_i est strictement supérieure au coefficient K_i de la borne K , alors on produit une nouvelle variable aléatoire S_i ,

E33_12 : on répète l'étape E33_11 jusqu'à ce que la variable aléatoire S_i soit inférieure au coefficient K_i de la borne K , puis on égalise le coefficient R_i à la variable aléatoire S_i .

Dans un tel mode de réalisation, tous les coefficients R_i obtenus sont des nombres directement produits par le générateur hardware de nombres aléatoires, ces coefficients sont donc parfaits et le nombre R qui en résulte est également parfait. en d'autres termes, la distribution obtenue des nombres R est uniforme dans l'intervalle $[0, K]$.

Selon un deuxième mode de mise en œuvre, au cours de l'étape E33, on choisit le coefficient R_i de rang i égal à une partie de la variable aléatoire S_i , partie inférieure au coefficient K_i . La dite partie correspondant dans un exemple à un nombre limité de bits de la variable S_i .

Selon un troisième mode de réalisation, au cours de l'étape E33, on réduit la variable aléatoire S_i modulo K_i+1 , le résultat de la réduction étant le coefficient R_i cherché.

Ces deux derniers modes de réalisation sont rapides par rapport aux procédés connus, essentiellement parce qu'on travaille sur des petits nombres. Les distributions de nombres aléatoires obtenus ne sont cependant pas uniformes : le simple fait de tronquer la variable S_i ou d'effectuer une réduction modulo K_i+1 introduit

nécessairement un biais. Toutefois, ce biais est moindre par rapport aux procédés de l'art antérieur.

Par ailleurs, il est possible de réduire le biais des procédés selon les deuxième et troisième modes de réalisation proposés, comme on va le voir ci-dessous.

Dans un procédé selon l'invention tel que décrit ci-dessus, on construit un nombre aléatoire R inférieur à K à partir de variables S_i de taille N produits par un générateur physique parfaitement aléatoire. Le nombre R obtenu est biaisé, mais le biais est réduit par rapport à un procédé connu.

Pour cela, dans le deuxième mode ou le troisième mode de réalisation, on construit notamment au cours de l'étape E33_1 un coefficient $R_i \leq K_i$ à partir de variables S_i de taille N . Pour réduire le biais introduit sur le coefficient R_i , on propose de le construire en utilisant les mêmes étapes E1 à E3 que pour construire le nombre R . En quelque sorte, on "imbrique" deux procédés similaires. Ceci permet de réduire encore la taille des nombres sur lesquels on travaille, et en conséquence de réduire encore le biais sur les coefficients de R , et sur le nombre R final.

Concrètement, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33_1), on exécute les étapes E1 à E4 en utilisant une base $(\beta^{q-1}, \dots, \beta^0)$ comme base de calcul, β étant un nombre entier strictement inférieur à W et q étant le degré de K_i dans la base β .

L'étape E33 est ainsi décomposée en les sous-étapes suivantes :

E33_41 : on décompose le coefficient K_i de rang i de la borne K dans la base $(\beta^{q-1}, \dots, \beta^0)$ ($K_i = \sum_{j=0}^{q-1} (K_i)_j * \beta^j$ ou $K_i = (K_i)_{q-1} \dots (K_i)_1 (K_i)_0$), j étant un indice de boucle, $(K_i)_j$ étant un nombre compris entre 0 et $\beta-1$ et q étant un degré du coefficient K_i ,

E33_42 : on initialise à VRAI une deuxième variable booléenne g ,

E33_43 : on réalise les opération suivantes, dans une boucle indicée par j variant entre $q-1$ et 0:

E33_431 : on produit une variable aléatoire $(S_i)_j$ comprise entre 0 et $\beta-1$,

E33_432 : si la variable aléatoire $(S_i)_j$ est strictement inférieure au coefficient $(K_i)_j$, alors on met à FAUX la deuxième variable booléenne g ,

E33_4331 : si la variable aléatoire $(S_i)_j$ est strictement supérieure au coefficient $(K_i)_j$ et si la deuxième variable booléenne g est VRAI, alors on détermine un coefficient $(R_i)_j$ à partir de la variable aléatoire $(S_i)_j$ selon une fonction prédéfinie,

E33_4332 : sinon, poser $(R_i)_j = (S_i)_j$

E33_434 : on décrémente l'indice de boucle j ,

E33_44 : on détermine le nombre aléatoire R_i par recombinaison des coefficients aléatoires $(R_i)_j$ dans la base β ($R_i = \sum_{j=0}^{q-1} (R_i)_j * \beta^j$ ou $R_i = (R_i)_{q-1} \dots (R_i)_1 (R_i)_0$).

Comme on vient de le voir ci-dessus, en "imbriquant" deux procédés, on réduit le biais des nombres aléatoires R produits par le procédé global, tout en conservant un procédé global rapide. On peut bien sûr imaginer d'"imbriquer" plus de deux procédés, par exemple trois ou quatre, en décomposant, dans l'étape E33_43 les nombres

dans une base $\gamma < \beta$, et en décomposant l'étape E33_43 en une succession d'étapes similaires aux étapes E33_41 à E33_43.

De manière générale, plus on "imbrique" de procédés, plus les nombres sur lesquels on travaille sont petits : la durée de chaque étape diminue et le biais des nombres produits par le procédé global diminue également.

L'invention a également pour objet un composant électronique adapté pour la mise en oeuvre d'un procédé tel que décrit ci-dessus. Un tel composant comprend notamment un générateur produisant des nombres aléatoires de taille N, et des circuits de calcul pour réaliser des opérations sur des nombres de au plus N bits.

Selon le mode de réalisation du procédé à mettre en oeuvre, les circuits de calcul sont adaptés pour réaliser des opérations de comparaison de deux nombres, de troncature de nombre, de réduction modulaire.

Le générateur de nombres aléatoires et les circuits de calcul sont pilotés de préférence par un moyen logiciel mémorisé dans une mémoire du composant prévue à cet effet.

L'invention concerne également une carte à puce comprenant un composant électronique tel que décrit ci-dessus.

REVENDEICATIONS

1. Procédé cryptographique, au cours duquel on utilise un générateur de nombres aléatoires produisant des nombres aléatoires S_i de taille N fixée compris entre 0 et $W-1$, pour produire un nombre aléatoire R compris entre 0 et une borne K prédéfinie, caractérisé en ce que :

E31 : on produit une variable aléatoire S_i comprise entre 0 et $W-1$,

E32 : si la variable aléatoire S_i est strictement inférieure à un coefficient K_i de la borne K dans la base W , alors le coefficient R_i de rang i du nombre aléatoire R est égal à la variable aléatoire S_i puis, pour tout rang j inférieur à i , on produit une variable aléatoire S_j entre 0 et $W-1$ et on pose $R_j = S_j$.

E33 : sinon, si la dite variable aléatoire est supérieure au coefficient K_i de rang i de la borne K dans la base W , alors on détermine le dit coefficient R_i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie, puis on détermine le coefficient R_{i-1} du nombre aléatoire R de rang $i-1$ immédiatement inférieur en répétant les étapes E31 à E33.

2. Procédé selon la revendication 1, au cours duquel on réalise les étapes suivantes :

E1 : on décompose la borne K dans une base $(W^{p-1}, W^{p-2}, \dots, W^0)$ sous la forme $K = \sum_{i=0}^{p-1} K_i * W^i$, i étant un indice de boucle, K_i étant un coefficient de la borne K de rang i compris entre 0 et $W-1$ et p étant le degré de la borne K ,

E2 : on initialise à VRAI une variable booléenne f,

E3 : on réalise les opération suivantes, dans une boucle indicée par i, i étant un nombre entier variant entre p-1 et 0:

E31 : on produit une variable aléatoire S_i comprise entre 0 et W-1,

E32 : si la variable aléatoire S_i est strictement inférieure au coefficient K_i de rang i, alors on met à FAUX la variable booléenne f,

E33_1 : si la variable aléatoire S_i est strictement supérieure au coefficient K_i de rang i et si la variable booléenne f est VRAI, alors on détermine le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i selon une fonction prédéfinie,

E33_2 : sinon, on pose $R_i = S_i$

E34 : on décrémente la variable de boucle i,

E4 : on détermine le nombre aléatoire R par recombinaison des coefficients aléatoires R_i dans la base W selon la

$$\text{relation : } R = \sum_{i=0}^{p-1} R_i * W^i.$$

3. Procédé selon la revendication 2, au cours duquel, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étapes E33_1 et E33_2), on réalise les sous-étapes suivantes :

E33_11: si la variable aléatoire S_i est strictement supérieure au coefficient K_i de la borne K, alors on produit une nouvelle variable aléatoire S_i ,

E33_12 : on répète l'étape E33_11 jusqu'à ce que la variable aléatoire S_i soit inférieure au coefficient K_i de la borne K, puis on égalise le coefficient R_i à la variable aléatoire S_i .

4. Procédé selon la revendication 2, au cours duquel, on choisit (étapes E33-1 et 33_2) le coefficient R_i de rang i égal à une partie de la variable aléatoire S_i , partie inférieure au coefficient K_i , la dite partie correspondant par exemple à un nombre limité de bits de la variable S_i .

5. Procédé selon la revendication 2, au cours duquel, au pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33), on réduit la variable aléatoire S_i modulo K_i+1 , le résultat de la réduction étant le coefficient R_i cherché.

6. Procédé selon l'une des revendications 1 à 5, au cours duquel, pour déterminer le coefficient R_i de rang i à partir de la variable aléatoire S_i de rang i (étape E33), on exécute les étapes E1 à E4 en utilisant une base $(\beta^{q-1}, \dots, \beta^0)$ comme base de calcul, β étant un nombre entier strictement inférieur à W et q étant le degré de K dans la base β .

7. Procédé selon la revendication 6, dans lequel l'étape E33 est décomposée en les sous-étapes suivantes :

E33_41 : on décompose le coefficient K_i de rang i de la borne K dans la base $(\beta^{q-1}, \dots, \beta^0)$ sous la forme

$$K_i = \sum_{j=0}^{q-1} (K_i)_j * \beta^j, \text{ } j \text{ étant un indice de boucle, } (K_i)_j \text{ étant}$$

un nombre compris entre 0 et $\beta-1$ et q étant le degré du coefficient K_i ,

E33_42 : on initialise à VRAI une deuxième variable booléenne g ,

E33_43 : on réalise les opération suivantes, dans une boucle indicée par j variant entre $q-1$ et 0:

E33_431 : on produit une variable aléatoire $(S_i)_j$ comprise entre 0 et $\beta - 1$,

E33_432 : si la variable aléatoire $(S_i)_j$ est strictement inférieure au coefficient $(K_i)_j$, alors on met à FAUX la deuxième variable booléenne g ,

E33_4331 : si la variable aléatoire $(S_i)_j$ est strictement supérieure au coefficient $(K_i)_j$ et si la deuxième variable booléenne g est VRAI, alors on détermine un coefficient $(R_i)_j$ à partir de la variable aléatoire $(S_i)_j$ selon une fonction prédéfinie,

E33_4332 : sinon, poser $(R_i)_j = (S_i)_j$

E33_434 : on décrémente l'indice de boucle j ,

E33_44 : on détermine le nombre aléatoire R_i par recombinaison des coefficients aléatoires $(R_i)_j$ dans la base β selon la relation : $R_i = \sum_{j=0}^{q-1} (R_i)_j * \beta^j$.

8. Composant électronique comprenant un générateur de nombres aléatoires de taille N , des circuits de calcul réalisant notamment une comparaison, une troncature et / ou une réduction modulaire sur des nombres de au plus N bits, et un moyen de pilotage du générateur de nombres aléatoires et des circuits de calcul, le dit moyen de pilotage étant adapté pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 7.

9. Carte à puce comprenant un composant électronique selon la revendication précédente.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2004/050510

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F7/58

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 966 313 A (SAKAMOTO HIDEKI) 12 October 1999 (1999-10-12)	1,6
A	abstract column 1, line 5 - line 21 column 3, line 1 - line 42 column 4, line 1 - column 5, line 63	2-5, 7-9
A	L'ECUYER P: "Uniform Random Number Generators: A Review" PROCEEDINGS OF THE WINTER SIMULATION CONFERENCE. ATLANTA, DEC. 7 - 10, 1997, NEW YORK, IEEE, US, 7 December 1997 (1997-12-07), pages 127-134, XP010258514 ISBN: 0-7803-4278-X page 128, right-hand column - page 192, right-hand column	1-9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

16 March 2005

Date of mailing of the international search report

05/04/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Bec, T

Information on patent family members

PCT/FR2004/050510

Form PCT/ISA/210 (patent family annex) (January 2004)

BEST AVAILABLE COPY **Best Available Copy**

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR2004/050510

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/58

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, PAJ, WPI Data, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 5.966 313 A (SAKAMOTO HIDEKI) 12 octobre 1999 (1999-10-12)	1,6
A	abrégé colonne 1, ligne 5 - ligne 21 colonne 3, ligne 1 - ligne 42 colonne 4, ligne 1 - colonne 5, ligne 63	2-5, 7-9
A	L'ECUYER P: "Uniform Random Number Generators: A Review" PROCEEDINGS OF THE WINTER SIMULATION CONFERENCE. ATLANTA, DEC. 7 - 10, 1997, NEW YORK, IEEE, US, 7 décembre 1997 (1997-12-07), pages 127-134, XP010258514 ISBN: 0-7803-4278-X page 128, colonne de droite - page 192, colonne de droite	1-9

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *Z* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

16 mars 2005

Date d'expédition du présent rapport de recherche internationale

05/04/2005

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Bec, T

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No

PCT/FR2004/050510

Formulaire PCT/ISA/210 (annexe familles de brevets) (Janvier 2004)

BEST AVAILABLE COPY